UNITED STATES DISTRICT COURT

MIDDLE DISTRICT OF TENNESSEE

UNITED STATES OF AMERICA
V.
Steven K. Gilmore

CRIMINAL COMPLAINT

Case Number: 09-4010-JSB

(Name and Address of Defendant)

I, the undersigned complainant state that the following is true and correct to the best of my knowledge and belief. On or about March 17, 2009 (Date) in Davidson County, in the Middle District of Tennessee defendant(s) did,

(Track Statutory Language of Offense)

knowingly and with intent to defraud possessed fifteen or more unauthorized access devices.

in violation of Title 18 United States Code, Section(s) 1029(a)(3).

I further state that I am a(n) Special Agent of U.S. Secret Service (Official Title) and that this complaint is based on the following facts:

See Attachment A

Continued on the attached sheet and made a part of this complaint: ☒ Yes ☐ No

Signature of Complainant

Matthew Stephenson

Printed Name of Complainant

Sworn to before me and signed in my presence,

4/1/2009
Date

at Nashville, Tennessee
City State

John S. Bryant
Name of Judge

U.S. Magistrate Judge
Title of Judge

Signature of Judge

ATTACHMENT A

AFFIDAVIT IN SUPPORT OF COMPLAINT

I, Matthew Stephenson, declare under penalty of perjury that the following is true and correct:

Introduction

1. I am a Special Agent with the United States Secret Service ("USSS") assigned to the Nashville Field Office, and have been employed as a Secret Service Agent for over nine years.

2. As part of my official duties, it is my responsibility to investigate access device card fraud and identity theft. Title 18, United States Code, Section 1029(a)(3) provides that it is unlawful to knowingly and with the intent to defraud possess fifteen or more unauthorized access devices.

3. Title 18, United States Code Section 1029(e)(1) defines "access device" to mean any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).

4. Title 18, United States Code, Section 1029(e)(3) defines "unauthorized access device" to mean any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud.

5. This affidavit is submitted in support of a Criminal Complaint and in support of an Application for a Search Warrant authorizing a search of the residential premises located at 2202D Cabin Hill Road, in Nashville, Tennessee.

6. The information contained in this affidavit is based upon information provided to me by Special Agent Joseph E. Craig of the Tennessee Bureau of Investigation and Special Agent Lee Eaves of the United States Secret Service, a computer investigative specialist. As explained below, I have probable cause to believe that Steven K. Gilmore has trafficked in stolen names, social security numbers, dates of birth and bank account information that he obtained when he was employed by Policy Studies, Inc. to assist with child support collection services for the Twentieth Judicial District of Tennessee. Mr. Gilmore was terminated from that position on January 8, 2009.

7. This investigation began on December 21, 2007, when an individual complained to the Trousdale County, Tennessee Sheriff's Office that his debit card had been used without his permission to pay for background checks on an individual named Michael Atkins.

8. On January 4, 2008, Detectives Kit Jenkins and David Winnett of the Trousdale County Sheriff's Office interviewed Anthony Michael Atkins. Mr. Atkins previously had been convicted of access device fraud in violation of Title 18, United States Code Section 1029(a)(2) in the Middle District of Tennessee on May 3, 2005. (See United States v. Atkins, Docket Number 2:04-cr-00018, Judgment, Docket Entry # 56). Mr. Atkins was on federal supervised release at the time he was interviewed by Detectives Jenkins and Winnett. Mr. Atkins advised Detectives Jenkins and Winnett that he had wanted to get a job at Nashville Cares, but was concerned that they would find out about his federal conviction. Mr. Atkins said that he asked an acquaintance named Steven K. Gilmore for a name similar to his own that he could use for an employment application. Mr. Atkins advised that Mr. Gilmore was then employed by Policy Studies, Inc. a Colorado-based company that contracted with the Tennessee Department of Human Services to provide child support enforcement services in the Twentieth Judicial District of Tennessee. As part of that job, Mr. Gilmore had access to personal identification information for residents of Tennessee and other states. Mr. Atkins said that Mr. Gilmore provided him with the name of Michael Ryan Atkins, who had a date of birth similar to that of Mr. Atkins. Mr. Atkins said that another friend of his used a credit card obtained from a customer of the restaurant where they both worked to pay for background checks run on the name of Michael Ryan Atkins. Mr. Atkins also told Detectives Jenkins and Winnett that Mr. Gilmore could get as many as one thousand identities at a time through his employment at Policy Studies, Inc., including names, dates of birth, social security numbers, addresses, address histories, and drivers license information.

9. On January 11, 2008, Detective Jenkins, Detective Winnett and District Attorney General Thomas P. Thompson, Jr. of the Fifteenth Judicial District of Tennessee, met with Special Agent Cindy Purviance and Special Agent-in-Charge Rus Winkler of the Tennessee Bureau of Investigation and relayed to them the information provided by Mr. Atkins about Mr. Gilmore.

10. On January 14, 2008, Agent Pruviance and Special Agent Roy Copeland of the Tennessee Bureau of Investigation interviewed Mr. Atkins at the Office of the District Attorney General in Lebanon, Tennessee. Detectives Jenkins and Winnett also were present. During that interview, Mr Atkins advised that he had known Mr. Gilmore for approximately four years. Mr. Atkins advised that before Mr. Gilmore worked for Policy Studies, Inc. that he had worked for the Child Support Division of the Office of the District Attorney General in Cookeville, Tennessee. During the time that Mr. Gilmore was employed by the District Attorney's office, he had provided personal identification information to Mr. Atkins. Mr. Atkins stated that since Mr. Gilmore had worked for Policy Studies, Inc. that he had provided personal identification information to Mr. Atkins on about a half dozen occasions. Mr. Atkins stated that he typically received five to ten identities from Mr. Gilmore on each occasion. These identities included names, dates of birth, addresses, and driver's license information. Mr. Gilmore sent this information to Mr. Atkins via email messages. Mr. Gilmore charged Mr. Atkins $2 to $3 for each set of personal identification information that he sold to Mr. Atkins. Mr. Atkins said that Mr. Gilmore had access to multi-state databases

at Policy Studies, Inc., but that he had access to more detailed information for Tennessee residents. Mr. Atkins advised that Mr. Gilmore also had access to Tennessee employment records.

11. On February 13, 2008, Agent Purviance and Agent Copeland met again with Mr. Atkins and his federal public defender pursuant to a proffer agreement between Mr. Atkins and the United States. Mr. Atkins advised that he first met Mr. Gilmore while attending Tennessee Technological University in Cookeville, Tennessee. At that time Mr. Gilmore worked for the District Attorney's Office in Putnam County, Tennessee and had access to personal information databases for Tennessee residents. In about 2003, Mr. Atkins first asked for and purchased several identifications from Mr. Gilmore. Mr. Atkins stated that he obtained information from Mr. Gilmore on three or four separate occasions, possibly more. The amount of information that he received each time would last Mr. Atkins for a couple of months. Mr. Atkins used this information to open fraudulent Ebay seller accounts using the identities given to him by Mr. Gilmore. Mr. Atkins then used the fraudulent Ebay seller accounts to offer items for sale that he never owned and never intended to deliver. Each time his illegal activities were discovered by Ebay, Mr. Atkins used a new false identity to open a new fraudulent Ebay account. Mr. Atkins engaged in this fraudulent scheme for approximately one year until he was arrested in June of 2004. During this scheme, Mr. Atkins estimated that he purchased approximately fifty sets of information from Mr. Gilmore, each included a name, address, date of birth, drivers license number and social security number. After his first arrest, Mr. Atkins stopped purchasing identities for a period

of time. Mr. Atkins said that he resumed purchasing information from Mr. Gilmore in about 2005. He estimated that he purchased 10 to 15 sets of formation from Mr. Gilmore in 2005 on a couple of occasions. Mr. Atkins stated that Mr. Gilmore would charge from $2 to $5 for each set of information and would send him a bill through PayPal, an Internet base billing and payment system. Mr. Atkins stated that he either paid the bill through PayPal or would take Mr. Gilmore out for drinks to settle the debt. The personal identification information supplied to Mr. Atkins by Mr. Gilmore was sent to Mr. Atkins via email. The information usually was sent to Mr. Atkins from Mr. Gilmore's email account, happyskg2@yahoo.com. Mr. Gilmore personally delivered information to Mr. Atkins on approximately two occasions. In around May of 2007, Mr. Atkins discussed with Mr. Gilmore his concern that a prospective employer would run a background check and discover Mr. Atkins' criminal history. According to Mr. Atkins, Mr. Gilmore suggested that Mr. Atkins use the social security number of someone with a similar name. Between about October and December of 2007, Mr. Gilmore provided names to Mr. Atkins that he could use to apply for employment.

12. Following the meeting on February 13, 2008, the United States sought and obtained federal court approval for Mr. Atkins to assist law enforcement in an investigation of Mr. Gilmore while he remained on supervised release.

13. On October 9, 2008, Special Agent Joseph Craig of the Tennessee Bureau of Investigation directed Mr. Atkins pay $25 to Mr. Gilmore for five sets of personal identification

information, including names, social security numbers and dates of birth, sent to Mr. Atkins via email by Mr. Gilmore on that date. This meeting between Mr. Atkins and Mr. Gilmore was recorded.

14. On October 22, 2008, Agent Craig directed Mr. Atkins request ten more sets of personal identification information from Mr. Gilmore. Ten more sets of personal identification information, including names, social security numbers and dates of birth, were sent to Mr. Atkins via email by Mr. Gilmore on that date. On October 30, 2008, Mr. Atkins met with Mr. Gilmore at his office in the Metro Center complex and paid him $100 for the ten sets of information. This meeting between Mr. Atkins and Mr. Gilmore also was recorded.

15. On about January 15, 2009, Mr. Atkins advised Agent Craig that Mr. Gilmore had been terminated from his employment with Policy Studies, Inc. However, Mr. Atkins advised Agent Craig that he believed that Mr. Gilmore still had sets of personal identification information for sale. Shortly after that, Mr. Atkins advised Agent Craig that Mr. Gilmore still had approximately 1,500 to 2,000 sets of personal identification information available for sale. Agent Craig asked Mr. Atkins to inquire whether Mr. Gilmore had access to any bank account information. Mr. Atkins subsequently advised Agent Craig that Mr. Gilmore said he had about 1,500 sets of identities that included bank account information.

16. On March 17, 2009, Mr. Gilmore sent Mr. Atkins an email containing twenty more sets of personal identification information and one copy of an Administrative Order for Seizure of

Assets that appeared to be a record of the Tennessee Department of Human Services. That Administrative Order contained the bank account number and social security number for an individual whose assets were subject to seizure for payment of back child support. On March 18, 2009, Mr. Atkins again met with Mr. Gilmore and paid him $100 for the twenty sets of personal identification information. This meeting between Mr. Atkins and Mr. Gilmore also was recorded.

17. On March 30, 2009, Mr. Atkins brokered an agreement for Mr. Gilmore to sell his complete database, which Mr. Gilmore claims contains approximately 1,600 sets of personal identification information, to Agent Craig acting in an undercover capacity for $2,800. This transaction is expected to take place on the afternoon of Wednesday, April 1, 2009. Mr. Gilmore has advised Mr. Atkins that he will deliver the 1,600 sets of personal identification information on a flash drive.

18. Agent Craig also has learned that on about February 3, 2009, Mr. Gilmore applied for employment with the child support services division of the District Attorney's Office in Wilson County, Tennessee. The coordinator for that office happened to be the spouse of Agent Copeland and fortuitously learned from Agent Copeland and Agent Craig that Mr. Gilmore was under investigation by the Tennessee Bureau of Investigation. Agent Craig obtained the resume that Mr. Gilmore had submitted to that office. That resume reflects that Mr. Gilmore resides at 2202D Cabin Hill Road, Nashville, Tennessee 37214. Agent Craig has driven to that address. The premises at that address consist of a two story duplex with

blue siding and cream colored trim. It has a wood privacy fence around the back yard. The house number "2202D" appears on a post that supports a small roof over the doorway at the side entrance to the duplex. That entrance is on the right side of the duplex as you face it from the street.

19. From the foregoing it appears that at least one computer has been used by Mr. Gilmore as an instrumentality in the course of, and in furtherance of the sale of stolen personal identification information. Moreover, it is reasonable to believe that records and evidence are being stored in electronic form on computer hard-drives, disks, CDs, thumb drives, flash drives and other similar electronic storage devices.

20. It also appears from the foregoing facts, that computer hardware has been used by Mr. Gilmore to save records and for communications. Programs loaded on the drives of computers are the means by which the computer can send and save those file records and communications. Password and security devices are often used to restrict access to or hide computer software, documentation or data. Each of the component parts of a computer thus are integrated into its entire operation. In order to best evaluate the evidence, the computers -- and all of the related computer equipment used with the computers -- should be available to a computer investigator/analyst.

21. In addition to the need to have all of the components available when a search of the computer is undertaken, the search of the computer itself is a time consuming process. Unlike the

search of documentary files, computers store data in "files" which cannot easily be reviewed. For instance, a single 2 gigabyte hard-drive is the electronic equivalent of approximately 1,000,000 pages of double-spaced text. Furthermore, software and individual files can be "password" protected; files may be secluded in hidden directories; files can be mislabeled or be labeled with names which are misleading; similarly, files which contain innocent-appearing names ("Smith.ltr") may actually be electronic commands to electronically self-destruct the computer; files can also be "deleted" -- but unlike documents which are destroyed -- - "deleted" electronic files remain on the storage device until randomly "written over" by the computer.

22. For example, a computer's hard-drive typically stores information in a series of "sectors" each of which contain a limited number of electronic bytes - usually 512. There are thousands of such sectors on the hard-drive and the computer jumps randomly among the sectors when storing a particular file. Thus, a portion of a memo could be at Sector 103 while the next portion of the memo could be stored at Sector 2057. When retrieving the memo, the computer knows where to find the next appropriate sector because of information supplied to it at the end of the last sector. If the memo had been "deleted", the only thing initially removed is the "label" information at the beginning of the first sector. The remaining sectors are not erased until a new file is "saved" and then the computer may or may not select the "old memo" sectors, as it randomly looks for available sectors in which to store the new file.

23. Being aware of these pitfalls, the investigator/analyst must follow a time-consuming procedure to review the contents of the computer and the computer-related equipment so as to insure the integrity of the data and/or evidence. Even if a deleted file has been overwritten and no fragment remains, applications which provide access to the internet and also operating systems maintain records (or logs) of activity on the internet for an indefinite period of time. Such logs are located in directories not usually used and/or accessed by computer users. A single computer and related equipment could take many days to properly analyze.

24. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten.

25. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically

downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular operating system, storage capacity, and computer habits.

26. Accordingly, there is a reasonable need to remove the computers and computer-related equipment as instrumentality(ies) of the crimes and also to remove the computers to a forensically-secure location in order to properly conduct a thorough search of their contents, so as to determine if any of the authorized information/data is located therein. Such action will greatly diminish the intrusion of law enforcement into the premises and will ensure that evidence can be searched for without the risk of losing, destroying or missing the information/data for which there has been authorization to search.

27. Therefore, it is respectfully requested that the warrant sought by this application authorize the search and seizure for all "computer hardware," "computer software" and business records which are more fully set out and explained above.

28. Based upon the foregoing facts and upon on my experience and training, I have probable cause to believe that Steven K. Gilmore has committed the federal offense of access device fraud in violation of 18 U.S.C. § 1029(a)(3). I also have probable cause to believe that

evidence of these crimes is concealed within the premises located at 2202D Cabin Hill Road in Nashville, Tennessee 37214.

29. Therefore, I ask that an arrest warrant be issued for the arrest of Steven K. Gilmore for violation of Title 18, United States Code Section 1029(a)(3). I also ask that a search warrant be issued authorizing the search of the premises located at 2202D Cabin Hill Road in Nashville, Tennessee 37214, described more completely in Attachment A to the Application for Search Warrant and the seizure of the items of evidence described in Attachment B to the Application for Search Warrant.

Matthew Stephenson
Special Agent
United States Secret Service

Subscribed and sworn before me this 1st day of April, 2009

John S. Bryant
U.S. Magistrate Judge
Middle District of Tennessee